

**State of West Virginia**  
**Executive Branch**  
**INFORMATION SECURITY**  
**Strategic Plan**



*This plan was prepared by the Office of Information Security and Controls  
Jim Richards, Chief Information Security Officer*

(This page was intentionally left blank)

---

## Contents

Information Security Program.....	4
1. Security Policy Development .....	5
2. Privacy Partnership.....	6
3. Risk Management.....	7
4. Business Continuity Plans (*) .....	9
5. Disaster Recovery Plans .....	10
6. Security Operations Center (SOC) and Security Operations.....	11
7. Training and Culture .....	12
8. Information Security Management Emphasis.....	14
9. Audit Program .....	15
10. Certification and Accreditation .....	16
11. Incident Management and Computer Forensics.....	17
12. Funding .....	18
13. Team Development.....	19
14. Information Security Metrics .....	21
15. Outreach .....	22
16. Office of Technology Partners.....	24
17. West Virginia Information Security Principles.....	26

---

## Information Security Program

### Introduction



A well documented statewide program for Information Security is a blueprint for the protection of information that is entrusted to the Executive Branch agencies. This information enables government operations and the provision of government services to citizens. The intent of this Strategic Plan is to identify the key elements of the West Virginia Executive Branch security program, and to outline the initiatives that support each element.

The West Virginia Office of Technology (OT) has developed Executive Branch security standards, policies, and procedures for use by Executive organizations, as well as to provide best practices guidelines for all other state and local public sector organizations. With these policies as a framework, procedures portray specifically how the policies are implemented. Policies developed by Executive Branch agencies, that address IT or Information Security issues, may be more, but not less, stringent than those issued by the State Chief Technology Officer (CTO).

West Virginia must maintain compliance with legal and regulatory requirements. It is essential that the OT implement practical measures to protect the State's Information systems (and the associated data) from compromise. Best practices must be followed in order to safeguard **all** forms of information.



This enterprise approach to Information Security enables WV State Government to move forward in a coordinated and effective progression toward reduced risk.

The concept of "layered security" involves the use of controls and protections at every opportunity in the information system landscape. Some of the layers in an effective information security program include: Policies, technical controls (firewalls, access control lists in network equipment, anti-virus, spam filtering, WEB site blocking, encryption, event monitoring, vulnerability scanning, configuration and patch management, etc.), awareness training leading to cultural change in the user community (locking unattended workstations, protecting passwords, handling and conveying sensitive information with regard to its content, etc.), management emphasis on risk reduction, minimum required privileges and access, segregation of duties, auditing for policy and regulatory compliance, and adequate physical security policy compliance.

The OT has adopted the *ISO Information Security Standards* as the basis for defining the West Virginia Information Security objectives.

---

## 1. Security Policy Development

### Introduction

The OT has created a general security policy for the Executive Branch of State government. Agencies may establish more stringent policy enhancement, but duplication of content should be avoided. Each agency developing a security policy supplement must submit it to the OT for review. If necessary, procedures must be developed to specify how each policy is implemented. While policies are generally published for general consumption, procedures are frequently maintained as internal documents, as they often provide operational details that should not be known to the public, for security reasons.



---

### Initiatives



**Initiative 1: Periodically update the Executive Branch security policies and procedures**

**Initiative 2: Create additional targeted policies and procedures**

**Initiative 3: Review agency Information Security policies to ensure consistency, minimization of duplication, and compliance with the Executive Branch security standards**

## 2. Privacy Partnership



### Introduction

The Information Office of Security and Compliance (OISC) collaborates with the West Virginia Privacy Office with the goal that privacy concerns are properly addressed. It is essential that privacy and security be viewed as related challenges for the State, and that the policies and standards set by both Offices become “woven” to the cultural fabric of the Executive Branch.

---

### Initiatives

**Initiative 1: Provide security expertise to the Privacy Management Team and State Privacy Officers**

**Initiative 2: Collaborate with the Chief Privacy Officer on security and privacy concerns, such as incident prevention, preparedness, and response**

---

## 3. Risk Management

### Introduction



In all technology environments, there are numerous risks to Information Technology (IT) systems and the data residing on them.

Changing vulnerabilities and threats requires risk assessments that are ongoing and far-reaching, in continuously repeating cycles, identifying emergent risks, and implementing new risk mitigation strategies.

Risk is a relationship between value, threats, and vulnerabilities. In the absence of any value, threat, or vulnerability, no risk exists. Value of data tends to increase in most organizations, and since the complete elimination of threats and/or vulnerabilities is impossible, some risk will always exist. The reduction of externally-based threats is generally not possible, although many threats can be blocked if they are known. Focus and resources must therefore be directed primarily at the reduction of vulnerabilities. Threats must be identified and understood as much as possible, so the targets of these threats – the vulnerabilities – can be reduced. A unique threat is created by a culture that is not well educated in security awareness, or fails to adhere to policy and best practices to which they actually have been oriented. If a user makes a mistake, or intentionally violates policy, this user becomes a threat. In fact, this threat may statistically be more likely to cause an incident than all the potential malicious external threats, such as hackers. These internal threats must be addressed with training and elevated cultural expectations.

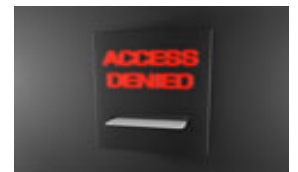
Resources available for the reduction of vulnerabilities are limited, so available resources should be allocated first to the vulnerabilities associated with highest value targets. Risk management starts with understanding what it is that has greatest value to the organization. For example, the State's most critical applications, and the data that these applications process.

In order to properly manage IT risks, the OT is utilizing a three step approach. The cycle is as follows:

- Risk Assessment
- Risk Mitigation
- Evaluation and re-assessment

Risk assessment is the initial phase in the risk management life-cycle. Risk assessment is used to determine each system's criticality to the entity (Department, agency, etc.), and to identify potential threats to each system. The output of this process seeks to identify appropriate controls for reducing or eliminating risk during the risk mitigation process. To determine the likelihood of a future adverse event, system threats must be analyzed in conjunction with potential vulnerabilities and other relevant factors.

The second process is risk mitigation. This involves evaluating, prioritizing, resourcing, and implementing the appropriate risk-reducing controls/countermeasures identified during the risk assessment process.



Components of the identified systems inevitably are upgraded or replaced, and software applications may be updated with newer versions or replaced. These changes can introduce new vulnerabilities, and previously mitigated risks can re-emerge, or new risks may materialize. Thus, the risk management process is ongoing and iterative, creating a repeating cycle of evaluation and re-assessment, followed by appropriate mitigation.

---

## **Initiatives (Risk Management)**

**Initiative 1: Review system characterizations: purpose, scope, criticality, platform, complexity, etc.**

**Initiative 2: Identify existing threats and vulnerabilities**

**Initiative 3: Analyze existing controls**

**Initiative 4: Determine likelihood and impact**

**Initiative 5: Create a risk matrix**

**Initiative 6: Conduct a cost-benefit analysis**

**Initiative 7: Determine a risk mitigation strategy based upon cost-benefit analysis**

**Initiative 8: Recommend changes in controls/countermeasures**

**Initiative 9: Complete mitigation activities**

**Initiative 10: Monitor system for changes and repeat process at appropriate intervals (go to: Initiative 1)**



---

## 4. Business Continuity Plans (\*)



### Introduction

Each agency is required to maintain **business continuity and / or Continuity of Operations (COOP)** plan for identified critical business functions. Each plan must specify how the agency will continue to sustain its critical business functions and provide services to constituent consumers until disrupted operations can be fully restored. Continuity plans must be tested and updated by the business units, in collaboration with the Office of Technology (to ensure technical feasibility of plans).

**(\*) Note:** The fact that Business Continuity Planning is included in this Strategic planning document does not in any way mean to suggest that this plan creation and maintenance can be accomplished by the OT or the OISC.

“Business Continuity Plans” is included in this document because it is our intent to monitor Continuity planning, since this planning is a necessary prerequisite to the disaster planning process that is performed by the IT organization (OT, etc.), and cannot be performed intelligently without a Business Continuity plan that identifies critical systems, and prioritizes the order of systems recovery.

Business Continuity planning must be performed by the business units, whose staff must have alternate working arrangements pre-planned in order to survive a crisis that renders the normal workplace unusable.

---

### Initiatives

**Initiative 1:** Assess status of agency data and system classification, to ensure adequate classification

**Initiative 2:** Working with agency leadership and selected continuity team members, ensure that viable business continuity plans are developed for each critical business function

**Initiative 3:** Ensure oversight focus upon achieving alignment between business continuity and disaster recovery plans

**Initiative 6:** Ensure periodic testing of business continuity, in conjunction with the associated disaster recovery plan

## 5. Disaster Recovery Plans

### Introduction



Disaster recovery plans may be developed with the thought that they will be useful only in the aftermath of explosions or natural disasters, but reliance on sound plans can be just as necessary when airborne asbestos is detected and causes a business location to become unusable. When an event occurs, disrupting normal business function, a rapid resolution is usually desired and expected, and for more critical functions, this resolution must necessarily be expedited. Disaster recovery addresses the requirement for restoring adequate IT functions when a significant or protracted interruption in service occurs.

Disaster recovery plans are technology service resumption plans derived from business continuity plans. This linkage ensures that restoration of a technology function is prioritized according to the business need(s). The recovery of IT functionality to meet the business need is the responsibility of the OT operational units. For this reason, disaster recovery requires a swift, coordinated effort undertaken by staff who may not typically work together under stressful urgency. Successful and efficient recovery can best be executed when the plan has been tested. The OT OISC is responsible for validating the completion, viability, and testing of these plans.

The OT Client Services, Networking and Enterprise Applications organizations may all play a key role in the recovery of IT services after a disruptive event. Client Services is taking the lead in the Disaster Recovery preparation activity, and has an individual(s) dedicated to this mission.

### Initiatives

**Initiative 1: Verify that disaster recovery plans are completed for each critical business function and aligned with the associated business continuity plan**

**Initiative 2: Ensure that each disaster recovery plan is aligned with the associated business continuity plan, where applicable**

**Initiative 3: Ensure adequate periodic testing and validation of disaster recovery plans is completed and documented**



---

## **6. Security Operations Center (SOC) and Security Operations**

### **Introduction**



To effectively reduce risk, a dynamic view of the traffic and “events” that take place in the State computing environment, including the network and the server farm, must be maintained. The SOC will be comprised of a set of tools that view events, correlate those that have anomalous characteristics, and intervene when traffic or events suggest that some errant or malicious activity is at work in the environment. When a problem is suspected, captured logs can be used to analyze event history, and the cause can be identified to a point in time and often a source location.

Security Operations includes the SOC activities, as well as vulnerability scanning of systems, validating patch levels, configuration hardening, and other system weaknesses.

---

### **Initiatives**

- Initiative 1: Develop the full functionality needed in the SOC, including traffic analysis, event correlation and log analysis, threshold alerts, etc.**
- Initiative 2: Maintain 24x7x365 security surveillance of network traffic and system events for all critical infrastructure components combining threat analysis and alerts to State technicians when any anomalies are detected, correlated, and/or quarantined.**
- Initiative 3: Maintain a regular schedule of vulnerability scanning within the State technical environment**
- Initiative 4: Develop geo-data displays that graphically represent Internet connections, traffic patterns, and highlight traffic that is suspicious by location or volume.**

---

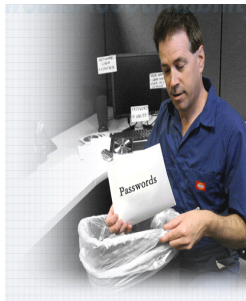
## 7. Training and Culture

### Introduction

People are often the weakest link in securing systems. Even the best technological and physical controls can be defeated easily if the human factor is weak. It is imperative that all State employees be part of the human defense system developed in the State.



This can only be accomplished with proper training and education that creates an elevated awareness of the threats, human vulnerabilities, and risk reduction techniques. To that end, the OT OISC deploys online Information Security awareness training. Topics include the following:



- Social Engineering – how to avoid being victimized by malicious manipulation techniques
- Password Management – creating, securing, and periodically changing strong, unshared passwords
- Physical Security – supporting controls in place to protect spaces, such as door controls
- Acceptable Use – avoiding unsafe or unethical use of State equipment
- Workplace Security – using precautions to prevent unauthorized access to systems/data
- Internet Security – web use and misuse issues; web filtering and malware challenges

The federal government enacted the *Computer Security Act of 1987* in response to Internet crime and cyber terrorism. This act requires periodic security awareness training for all federal employees who are involved in the management, use, or operation of a computer system. Making staff aware of threats has proven to be a very cost-effective countermeasure against security violations and/or mishaps. Gartner analysts Ouellet, Proctor, and Witty (2006) estimated that there is a 0.8 (\*) probability of 25% productivity savings in Information Security due to the workforce awareness of threats, risks, and controls, which reduces the number of security incidents. Staff trained in a security awareness program will have the knowledge to prevent common incidents and/or to reduce the damage done when an incident does occur.

All of the work involved in creating a set of technological system security controls (such as firewalls, anti-virus, encryption, etc.) is diminished in the absence of a comprehensive awareness training plan for all State employees.

(\*) 80%

## **Initiatives (Training and Culture)**



**Initiative 1: Provide all Executive Branch employees with security awareness training**

**Initiative 2: Establish an annual refresher training requirement for all employees**

**Initiative 3: Establish a process to assure completion of training and refresher sessions by all employees, with proper documentation of completion. This will also include new employees, contractors, and any other individuals using state computer systems**

**Initiative 4: Establish minimum training standards, and assist with curriculum development that addresses the unique and/or elevated responsibilities and requirement for expertise in the following roles:**

- 1. Management / Supervisory**
- 2. Technician**
- 3. Help Desk**
- 4. Mobile or Portable Device User**

**Initiative 5: Offer web based Information Security awareness training to local governments at no charge**

---

## 8. Information Security Management Emphasis



### Introduction

Under the authority established by Senate Bill 653, effective July 1, 2006, and the Governor's Executive Order 06-06, and following the mandate of these documents, a Senior Information Security Team, known as the Governor's Executive Information Security Team (GEIST) is in place to assist with the implementation of Information Security initiatives throughout the Governor's Executive Branch.

The membership of this team is comprised of the Information Security Administrators (ISA) appointed by the Cabinet Secretaries of each Department or agency. These ISAs provides leadership in the following areas:

- **Business Continuity planning**
- **Training completion tracking and documentation**
- **Risk management**
- **Data classification**
- **Plan testing**
  - **Business continuity and disaster recovery**
- **Audits**
  - **Facilitating Information Security audits performed by the OT OISC**
- **Policy implementation**
  - **Monitoring for compliance**
  - **Arranging emphasis or disciplinary action as needed**
- **Supplemental policy facilitation – Recommending policy additions, changes, or agency supplements to OT issued policy**
- **GEIST team membership and mandatory meeting attendance (or substitute attendance)**



---

### Initiatives

**Initiative 1: Maintain an informed and engaged GEIST through quarterly meetings, and adhoc meetings as needed**

## 9. Audit Program

### Introduction

Under the authority established by Senate Bill 653, effective June 11, 2006, and the Governor's Executive Order 06-06, the OT is charged with establishing an audit function to review compliance with all policy provisions that are issued concerning the use of technology, and the security practices governing that use. The OT OISC has undertaken this audit function with the establishment of the Audit Program. In addition to performing random or target audits in State Agencies, the Audit Program will review internal controls within the Office of Technology operations, and will conduct audits of selected 3rd party providers at their off-site locations.



### Initiatives

**Initiative 1: Conduct audits in agencies for compliance with Executive Branch IT policy, including the following:**



- User adherence to desktop practices of logging off workstations when leaving unattended, protecting passwords from use by others, and absence of confidential material left in plain view in the desktop area
- Absence of password sharing
- Adequate controls at building entrances and exits
- Documented completion of mandatory Information Security training
- Annual certification of working knowledge of policy governing Information Security practices
- Viability and testing of business continuity plan(s) with disaster recovery plan(s)

**Initiative 2: Conduct audits of technical environments, with emphasis on the OT, for compliance with policy and best practices related to the following:**

- Segregation of duties
- Unique administrative accounts for each technician with direct responsibility for a system function(s)
- Using administrative accounts for administrative duties only
- Maintaining current patch levels
- Using standard, policy-compliant, configurations (no default configurations in any device)
- Maintaining "least privilege" access rights for all users and technicians
- Using strong password enforcement controls on all systems



**Initiative 3: Formal reporting of findings to all levels of relevant management with recommendation for corrective action to mitigate identified risk(s)**

**Initiative 4: Conduct vulnerability scans, and perform penetration testing as needed to verify required system hardening.**

**Initiative 5: Contract for 3rd party auditing services to augment internal audit resources to perform additional audit services.**

**Initiative 6: Conduct audits of 3rd party provider agreements and services, potentially at their off-site locations, to ensure adequate security controls.**

## **10. Certification and Accreditation**

### **Introduction**

In the implementation of new software applications or the deployment of new hardware (servers, personal computers, wireless access points, etc.), it is critically important that the product being brought into production is correctly created and configured. Certification is a comprehensive validation and verification of the software or hardware, using rigorous testing, to ensure that security requirements have been met prior to introduction into the production environment. Accreditation is the approval and authorization to initiate any change in the technology environment within the scope of C and A.

The Certification and Accreditation is applied throughout the technology life-cycle to confirm that security controls are implemented correctly, and are effective in their implementation. While not all technology falls under the C and A umbrella, risk analysis should be applied to each technology being considered for deployment, to determine if this discipline is applicable.

Ultimately, the CTO should authorize the introduction of a piece of technology into the production environment, based upon its having met the applicable C and A standard for that technology.

---

### **Initiatives**

**Initiative 1: Establish the framework (process and procedure) for Certification and Accreditation, through a process of collaboration within the Office of Technology and between the OT and its State Agency partners.**

**Initiative 2: Define Certification and Accreditation criteria and scope, meaning, what kinds of technologies must undergo C and A before being moved into production.**

**Initiative 3: Plan, develop and deliver C and A training to all affected practitioners to foster the required cultural change, and provide necessary understanding about how to plan product and service rollouts within the C and A framework.**

**Initiative 4: Map C and A activities to the technology life-cycle.**

## 11. Incident Management and Computer Forensics

### Introduction



Incidents are inevitable, and the ongoing occurrences of incidents range in seriousness from mild to severe. With the frequency of reported incidents steadily increasing, the OISC must be proactive in its effort to protect all information and information systems from disruption, and maintain a readiness to recover from the effects of critical information security incidents. A proven incident management plan is recognized as the best preparation for the unexpected event.

The OT OISC creates policies, standards, and procedures to establish a framework specific to incident response. The OISC has established a central point of contact for reporting incidents ([incident@wv.gov](mailto:incident@wv.gov)), and an automated notification system to contact key responders. The OISC also offers consulting services and support during the analysis, recovery, and post-mortem phases of incident handling, to any State organization that is affected by a computer related incident with a security implication or impact.

Computer forensics capabilities are required to determine what has transpired in systems at a user level, in a server or network component, or on a system-wide level, after the fact. Forensics tools and skills may be employed to investigate computer abuse, an automated malware infestation or attack, or a targeted attack against any system. Forensics tools are also needed by our investigative and law enforcement partners, and we make our facilities, tools, and skills available to them as needed.

### Initiatives

#### Initiative 1: Maintain an Computer Security Incident Response Team (CSIRT)

- **Maintain appropriate policies and procedures for notification, response, and recovery from computer security incidents**
- **Maintain a central point of contact for reporting computer security incidents**
- **Maintain a service to provide alerts and notification of newly discovered computer vulnerabilities and threats to State, county and local government agencies**
- **Test the plan on a periodic basis; include testing of all the methods of establishing communications with critical responders**



**Initiative 2: Maintain suite of forensics tools and facilities where State Police and Special Investigations may also conduct forensics work, as needed**

**Initiative 3: Maintain adequate forensics skills to accomplish needed investigations professionally, timely, and suitable for evidence in a court of law**

---

## 12. Funding

### Introduction



The practice of Information Security and Compliance in the Executive Branch of West Virginia is an endeavor to prevent problems that are more costly than the expense of instituting preventative controls, including the cost of supporting the OISC's set of functions. For the most part, the OISC does not generate revenue, however there are exceptions. For this reason, operational cost must be borne by all Agencies in proportion to their use of IT services. In 2007, the cost of Information Security began to level off in many organizations, after multiple years of substantial spending to elevate security controls throughout the environment.

Investment in Information Security in the Executive Branch of West Virginia has historically been minimal. Pre-centralization of the Information Security and Compliance function within the OT, agencies had varying levels of concentration in this area, funded and focused proportionately to the perceived need of agency leadership.

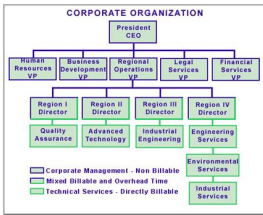
Staffing levels in the OT OISC will continue to increase somewhat over the coming years, through the consolidation of infrastructure into the OT, and by limited hiring into newly allocated positions. Increasing the mission of the OISC may require additional personnel resources above the levels portrayed in this document. Investment in appropriate tools, and maintenance of existing tools, to adequately perform policy development and maintenance, monitoring and auditing services, training, forensics, etc., will continue at an appropriate level of spend.

---

### Initiatives

**Initiative 1: Establish a per/seat user fee for security services that will fund a viable Information Security and Compliance program as described in this document**

## 13. Team Development



### Introduction

Staffing levels and building expertise with targeted training must be adequate to support the mission of the OISC, even as this mission grows, and the ongoing requirements of both the technical and administrative components of the OISC grow. While specialization and depth of skill levels is desirable, Information Security staff will be required to assume multiple roles, as they will at times participate in the audit program, policy development, training development and deployment, forensics, and research and testing functions, to name a few.

Each staff person will be cross trained, and acquire multiple skill-sets. We will collaborate as a team, and create time and task-defined “virtual teams” to complete specific projects, and to meet both short and long-term objectives.

A startup team is projected at nine staff, plus the Director, for a total of 10 full-time Information Security staff in the OISC. An expanded mission scope could require adjustments to this projected staffing plan.

Technical Security:	Three	FTE
Administrative Security:	Three	FTE
Policy Specialist:	One	FTE
Privacy/Special Projects	One	FTE
Administrative Support:	One	FTE



### Initiatives

**Initiative 1: Develop Job Classification Series that closely describes the work of an Information Security professional**

**Initiative 2: Secure resources needed to accomplish the goals of the OISC, and the initiatives set forth in this plan**

**Initiative 3: Acquire staff through absorption of consolidated staff, and through hiring as required**

**Initiative 4: Train and cross-train staff to a multi-disciplinary model as much as possible. Develop staff skills, professionalism, and business awareness, keeping career progression and succession planning in the skills development strategy**

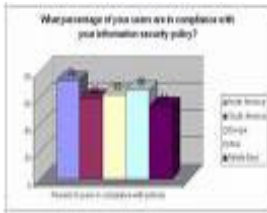
**Initiative 4: Identify “virtual team” leadership roles for the following:**

- Incident Management
- Forensics
- Training curriculum development and training/presentation delivery
- Liaison work with partner groups, such as:
  - Governor's Executive Information Security Team (GEIST)
  - Local government
  - Special Investigations (Legislative)
  - Law Enforcement
  - Internal OT Units: Networking, Client Services, Enterprise Application Development
  - External Application Development / WEB Development groups
- Disaster Recovery Oversight
- Audit Program
- Monitoring, Log Analysis, Event Correlation, IDS/IPS
- Policy/Procedure Development
- Security Emphasis Events/Activities
- Metrics
- Physical Security Liaison



**Initiative 5: Create virtual teams as needed to address functions in Initiative 4**

## 14. Information Security Metrics



### Introduction

In order to measure progress in our work, both as a factor of changing conditions, and changing capabilities, and to be able to represent “where we are” to stakeholders, we need to refine a system of capturing and reporting metrics. The types of metrics needed will vary by the audience for whom they are developed. The audience should ideally have a role in prescribing the metrics that are most useful to them.

### Initiatives

- Initiative 1: Work with a representation of partners to develop a set of metrics to be identified and tracked. Determine the interval, frequency, and format for reporting on these metrics to the various stakeholder groups**
- Initiative 2: Determine how to derive the metric, and most efficiently capture and report the metric at the specified interval**
- Initiative 3: Automate the metrics reporting function wherever possible**
- Initiative 4: Continue to evaluate the effectiveness of the metrics strategy**

Example Conversion Metrics

Category	User Status	Conv %	Est. Value
Acquisition	Visit Site (or landing page, or external widget)	100%	\$ .01
Acquisition	Doesn't abandon (leaves 2+ pages, stays 100 sec, 2+ clicks)	70%	\$ .05
Activation	Happy 1st Visit (leaves 3+ pages, stays 1 min, 2+ clicks)	30%	\$ .25
Activation	EmailSignup/SMS/Magnet Signal (providing email, phone, text to the web, etc)	5%	\$ 1
Activation	Asset Signup (uploading to web, etc)	2%	\$ 3
Retention	Email Open / RSS view or Downloads (in weeks or first 30 days)	3%	\$ 2
Retention	Repeat Visitor (in weeks or first 30 days)	2%	\$ 5
Referral	Refer 1+ users who visit site	2%	\$ 3
Referral	Refer 1+ users who activate	1%	\$ 10
Revenue	User generates minimum revenue	2%	\$ 5
Revenue	User generates break-even revenue	1%	\$ 25

---

## 15. Outreach



### Introduction

#### Public Sector Partners

The OISC is the leader in providing necessary Information Security services in West Virginia's Public Sector. It is therefore essential that we are willing to share the resources and talent developed within our organization to assist all of the West Virginia government entities in any effort they undertake to realize more effective Information Security practices. We are committed to be supportive of our fellow public sector partners, including law enforcement.

#### Physical Security Partners



Physical Security is the front line of defense in the practice of Information Security. If individuals with malicious intent are permitted to enter a State facility, their ability to do harm is significantly enhanced. The use of security badges, door controls, surveillance, and other physical controls are essential to effective physical security management. Under the current organizational structure in the Executive Branch, physical security is coordinated out of the Department of Military Affairs and Public Safety (DMAPS). For this reason, it is highly desirable for the OT OISC to maintain a strong working relationship with our physical security partners, such as the Division of Protective Services.

#### Other Security Partners

A critical aspect of maintaining an effective Information Security program is the exchange of intelligence and expertise among practitioners. The OT OISC is actively involved with multiple national organizations, and maintains relationships with other West Virginia State experts. In this capacity, the OT OISC acts as a conduit for Information Security alerts and advisories.



---

## Initiatives

- Initiative 1: Share expertise, assistance, and training materials with other public sector organizations**
- Initiative 2: Promote discussions that will enhance the security work of all public sector partners in West Virginia, including organizations such as the State Treasurer's Office, the Secretary of State, and State offices not within the Governor's span of authority, as well as counties and municipalities.**
- Initiative 3: Maintain active participation with the Multi State – Information Sharing Analysis Center (MS-ISAC), including focus committee participation (currently Training and Awareness, Outreach and Operations)**

---

## **Initiatives Continued (Outreach)**

- **Continue to update the State alert level and relay all advisories**
- **Maintain the membership list of members of the State of WV MS-ISAC Portal**

**Initiative 4: Maintain active participation in the National Association of State CIOs (NASCIO) Privacy and Security workgroup**

**Initiative 5: Maintain a working relationship with Legislative Special Investigations**

---

## 16. Office of Technology Partners



### Introduction

Looking from a security perspective across the State's technical landscape, it is a given that no organization needs greater security self-discipline than the OT itself. Our staff hold the "keys to the kingdom(s)," and have access to virtually every reach of the computing environment in West Virginia State government. With these elevated access privileges come equally elevated responsibilities, as well as the need for accountability throughout the technical organization.

It is important that all organizational units in the OT work closely together, and particularly closely with Information Security to ensure that we are creating and using standards in naming conventions, configurations, settings, documentation, and process creation and implementation. All of our initiatives and projects should have security objectives embedded within the architecture, and incorporated into the setup routine for all system components. Information Security should be involved as a partner in every design project, and should be an active participant in regular meetings with Client Services, Enterprise Applications, and Networking.

Each organization with a role in the technical setup and administration of system components should align their operational activities with the following fundamental security concepts:

- 1) Least Privilege – No assignment of privilege to anyone without a need for access
- 2) Segregation of Duties – Separation of responsibilities to ensure no conflict of interest, and to ensure accountability
- 3) Documentation of security activities – Diligence is not verifiable without documentation
- 4) Cross training to provide redundant skills in critical functional areas – Eliminate skills vulnerabilities
- 5) Documentation of all configurations and system setup procedures - In the event of a failure or "disaster," restore and recovery operations may need to be completed by someone other than the primary technician assigned to the system support function. Thorough documentation reduces dependence on single or specific individuals during critical situations.
- 6) Job Control – Techniques used to ensure that critical functions cannot be adversely impacted by a single individual. Can include mandatory paid time off, rotation of responsibilities and implementation of requirements for multiple individuals to perform key functions.

---

### Initiatives

**Initiative 1: Review all procurements processed by or through the OT having any technical, physical, or administrative security implications, for consistency and compatibility with overall security architecture technologies and strategies**

**Initiative 2: Maintain active participation in all substantive planning sessions within the OT and the Executive Branch, or specifically elect (cont.) to not participate, documenting the reason why.**



---

## Initiatives Continued (Office of Technology Partners)

- Initiative 3:** Monitor all security-related operational activities for compliance with best practices, policies, procedures, and standards, particularly in the five concept areas listed above.
- Initiative 4:** Maintain a comprehensive set of policies specifically addressing the expectations held for employees with critical technical roles, in view of their elevated privileges, and the inherent threat potential (e.g. non-malicious accidents) that elevated privilege provides to the holder.
- Initiative 5:** Develop specialized training for technicians addressing responsibilities and accountability practices, emphasizing the policies and procedures developed solely for their reference and compliance as privileged-access users within the State's technical infrastructure.
- Initiative 6:** Implement an Accreditation and Certification Program requiring compliance with all applicable standards including, but not limited to security standards, documented, with signoff, by an authorized authority (CTO or designee), prior to putting any system (hardware or software) into production within the Executive Branch (CTO's span of control). This applies to Servers, Personal Computers, PDA's, Thumb Drives, Applications, Networking components, and other devices that require setup or customization to work properly in the State environment with appropriate security settings enabled.

## 17. West Virginia Information Security Principles

- ❖ Security Awareness – All employees should understand the elements of their role in the protection of information systems and the data that these systems contain.
- ❖ Individual Responsibility – All employees should be responsible for their actions in the use of information systems, in order to support Information Security.
- ❖ Incident Prevention/Reporting – Employees should strive at all times to prevent security incidents, and report suspected incidents in a timely manner.
- ❖ Ethical Practices – All employees should adhere to the ethical standards established for public employees in their use of information systems.
- ❖ Respect – Employees should recognize the sensitivity of data maintained about citizens, and respect the confidentiality needs and rights of all individuals.
- ❖ Risk Awareness – As part of the larger risk awareness / risk management process, each employee should review and report any and all risks (threats or vulnerabilities) that may uniquely impact their specific work with information systems.
- ❖ Culture of Security – Employees should incorporate secure practices into all of their work activities, handling of information, and use of information systems.
- ❖ Security Leadership – All levels of leadership in West Virginia State government should support sound security practices, and respond constructively and comprehensively to all security initiatives.
- ❖ Process Improvement - Ongoing analysis and re-evaluation of risks, threats and vulnerabilities should foster continuous improvements in the security posture, and associated controls.